

Health Insurance Portability and Accountability Act (HIPAA)

1996

Why? What? Who? When? How?



WHY

HIPAA is federally mandated to:

- Improve portability & continuity of health insurance coverage.
- Combat waste, fraud, & abuse in health insurance & health care delivery.
- Simplify health insurance administration (administrative simplification).
- Promote use of medical savings accounts.
- Improve access to long-term care services & coverage.



WHAT

HIPAA Administrative Simplification consists of:

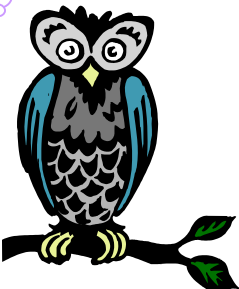
- Standardized electronic formats for healthcare business processes to improve efficiency – transactions and code sets.
- Standardized identifiers – providers, employers, health plans & individuals.
- Security requirements for data processing systems.
- Privacy protections for individual's health data.

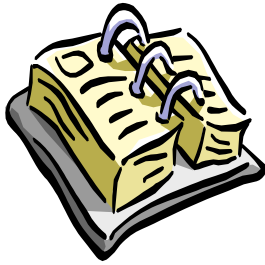
These are
the covered
entities.

WHO

HIPAA matters if you are one of the following:

- Health Plans – an individual or group plan that provides, or pays the cost of, medical care.
- Health Care Clearinghouses – an organization that translates non-standard health care data into standard formats or translates standard formats into non-standard formats on behalf of providers or health plans.
- Health Care Providers – a provider of medical or other health services, & any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
- Hybrid – a covered entity whose business activities include both covered & non-covered functions.



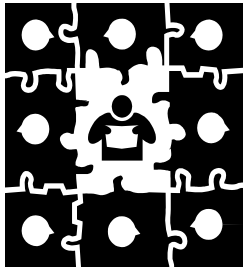


WHEN

Compliance dates are:

- Transactions and Code Sets: 10/03
- Privacy: 4/03
- Security: 5/05

HOW



Transaction set standards are enforced by HIPAA:

- If a health plan performs an affected business function (via any method), the health plan must be able to support the electronic standard for that transaction.
- If an electronic format is used, it must be in the mandated format according to the named implementation guide.
- Health plans cannot refuse to process transactions in the mandated format.
- Health plans cannot adversely affect trading partners who conduct business using the standards (e.g., charge a processing fee if services are free in other formats).

These are the HIPAA-compliant transaction sets and their associated standards for electronic transmission:

- Health Care Claim/Encounter or Coordination of Benefits - X12N 837
- Health Care Service Payment/Remittance Advice - X12N 835
- Health Claim Status Response/Request - X12N 276/277
- Eligibility Request/Response - X12N 270/271
- Provider Referral/Prior Authorization - X12N 278
- Enrollment in a Health Plan - X12N 834
- Health Plan Premium Payment - X12N 820
- Retail Pharmacy Claims or Prior Authorization - NCPDP

The following medical code sets are acceptable. Proprietary code sets can no longer be used. Non-medical code sets must use the values identified in the HIPAA implementation guides.

ICD-9-CM, Volumes 1 & 2	Diagnoses
CPT-4, HCPCS Level I	Physician Services
CDT	Dental Services
ICD-9, Volume 3	Inpatient Surgical Procedures
HCPCS Level II	Other Health Care Services
NDC	Drugs & Biologics (Retail Pharmacy)
No Standard Named	Drugs & Biologics (Non-Retail Pharmacy)



Privacy

Protected Health Information (PHI) includes all information that relates to:

- past, present, or future physical or mental condition of an individual;
- the provision of health care to an individual; or
- the past, present, or future payment for the provision of health care to an individual.

Permitted Uses and Disclosures:

Most uses of PHI within a covered entity fall under TPO.



- to the individual;
- for treatment, payment and operations (TPO);
- as required by law;
- with a written authorization.

Security

- Protects health data against unintended access.
- Protects the integrity of health data.
- Assures availability to authorized users.
- Encourages scalable solutions, what's best for an organization.

Examples:

- training of administrative procedures
- locking doors
- using passwords
- encrypting data

To start:

- Inventory PHI
- Assess security practices related to PHI